Docket No. 003239.P076
Express Mail No.: EL466330290US

UNITED STATES PATENT APPLICATION

FOR

REAL-TIME MEDIA COMMUNICATION OVER FIREWALLS USING A CONTROL PROTOCOL

INVENTOR:

LYNDON ONG

PREPARED BY:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 Wilshire Blvd., 7th Floor
Los Angeles, CA 90025-1026
(714) 557-3800

REAL-TIME MEDIA COMMUNICATION OVER FIREWALLS USING A CONTROL PROTOCOL

BACKGROUND

1. Field of the Invention

This invention relates to network communication. In particular, the invention relates to firewalls.

2. Description of Related Art

Currently, firewalls do not admit traffic which is not recognized. Most voice over Internet protocol (VoIP) traffic is not allowed across a firewall boundary because VoIP traffic contains no indication that the packet is VoIP and no indication of the originating and destination parties in the call. This limits VoIP service to service within a firewall-protected domain and does not allow users within the domain to call outside the domain and vice versa.

One existing technique is to add intelligence to firewall protocol so that the firewall can understand call signaling protocol (e.g., H.323) and can determine what Internet protocol (IP) address pair and UDP port pair to admit for a particular call. This technique has a number of drawbacks. First, the firewall is required to have significantly greater processing power and demands, resulting in high costs and integration efforts. Second, the firewall is required to be updated frequently as call signaling protocols change or are introduced, resulting in high maintenance and downtime costs. Third, the signaling is required to be processed by the firewall on every call, adding set-up delays and slowing down traffic.

Therefore, there is a need in the technology to provide an efficient technique for media communication via firewalls.

SUMMARY

The present invention is a method and apparatus to provide real-time media communication via firewalls. A real-time firewall includes a controller, a filter, and a modifier. The controller specifies a filtering characteristic based on a control protocol from a call server serving a firewall between source and a destination networks. The filter filters a packet in a call transmitted from the source network based on the filtering characteristic. The filter accepts the packet if the packet satisfies the filtering characteristic and rejects the packet otherwise.

According to one embodiment of the present invention, the controller further specifies a modifying action based on the control protocol. The real-time firewall further includes a modifier coupled to the controller and the filter to modify the accepted packet based on the modifying action. The modified packet is then sent to the destination network. The filtering characteristic may be at least one of a traffic characteristic, a network address, and a port identifier corresponding to the call.

The firewall in this invention may be able to do at least one of the following: (1) providing extensibility to existing firewall set-up, (2) allowing users within a firewall to call users outside firewall and vice versa, (3) increasing effective traffic management over firewall boundaries, and (4) accommodating real-time media communication over firewalls at low costs.

Other aspects and features of the present invention will become apparent to those ordinarily skilled in the art upon review of the following description of specific embodiments of the invention in conjunction with the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS

The features of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is a diagram illustrating a system in which at least one embodiment of the invention can be practiced.

Figure 2 is a diagram illustrating a real-time firewall according to one embodiment of the invention.

Figure 3 is a flowchart illustrating a process for real-time media communication across firewall according to one embodiment of the invention.

DESCRIPTION

A method and apparatus provides a technique for media communication across a firewall boundary in a network environment. In one embodiment of the invention, a real-time firewall includes a controller, a filter, and a modifier. The controller specifies a filtering characteristic based on a control protocol from a call server serving a firewall between a source and a destination networks. The filter filters a packet in a call transmitted from the source network based on the filtering characteristic. The filter accepts the packet if the packet satisfies the filtering characteristic and rejects the packet otherwise.

The firewall in this invention may be able to do at least one of the following: (1) providing extensibility to existing firewall set-up, (2) allowing users within a firewall to call users outside firewall and vice versa, (3) increasing effective traffic management over firewall boundaries, and (4) accommodating real-time media communication over firewalls at low costs.

In the following description, for purposes of explanation, numerous details are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that these specific details are not required in order to practice the present invention. In other instances, well-known electrical structures and circuits are shown in block diagram form in order not to obscure the present invention. For example, specific details are not provided as to whether the method is implemented in a station as a software routine, hardware circuit, firmware, or a combination thereof.

Embodiments of the invention may be represented as a software product stored on a machine-readable medium (also referred to as a computer-readable medium, a processor-readable medium, or a computer usable medium having a computer readable program code embodied therein). The machine-readable medium may be any type of magnetic, optical, or electrical storage medium including a diskette, compact disk read only memory (CD-ROM), memory device (volatile or non-volatile), or similar storage mechanism. The machine-readable medium may contain various sets of instructions, code sequences, configuration information, or other data. Those of ordinary skill in the art will appreciate that

other instructions and operations necessary to implement the described invention may also be stored on the machine-readable medium. Software running from the machine readable medium may interface with circuitry to perform the described tasks.

Figure 1 is a diagram illustrating a system 100 in which one embodiment of the invention can be practiced. The system 100 includes a public network 110, a private network 170, and a firewall 140.

The public network 110 is a public network external to the organization, e.g., the Internet. The public network 110 includes an end system 120 and a call server 130. The end system 120 is a system that receives or transmits a call or a message. Examples of the end system 120 include a computer, a call processing unit, a workstation, a private branch exchange (PBX), a telephony device, a wireless call unit. The end system 120 sends or receives real-time packets 152 to or from the firewall 140. In one embodiment, the real-time packets 152 may include real-time media information such as Voice over IP (VoIP), video, or audio/video. The call server 130 is a computer system that contains database, storage, processing power, switch and connection interfaces to other elements in the network 110. The call server 130 communicates with the end system 120 for a call setup, either during receiving and transmitting, using a call setup protocol 125. In addition, the call server 130 communicates with the firewall 140 using a control protocol 135.

The private network 170 is a network internal to the organization, e.g., an intranet. The private network 170 includes an end system 180 and a call server 190. The end system 180 is a system that receives or transmits a call or a message. Examples of the end system 180 include a computer, a processor, a central processing unit, a digital signal processing system, a call processing unit, a workstation, a private branch exchange (PBX), a telephony device, a wireless call unit, etc. The end system 180 sends or receives real-time packets 154 to or from the firewall 140. In one embodiment, the real-time packets 154 may include real-time media information such as Voice over IP (VoIP), video, or audio/video. The call server 190 is a computer system that contains database, storage, processing

power, switch and connection interfaces to other elements in the network 170. The call server 190 communicates with the end system 180 for a call setup, either during receiving and transmitting, using a call setup protocol 185. In addition, the call server 190 communicates with the firewall 140 using a control protocol 195.

At any time, the public network 110 may be transmitting or receiving a call to or from the network 170 via the firewall 140. Similarly, the private network 170 may be transmitting or receiving a call to or from the public network 110 via the firewall 140. A network that is transmitting information is a source network and a network that is receiving information is a destination network.

The firewall 140 is located between the networks 110 and 170. The firewall 140 includes a real-time firewall 150 and an application firewall 160. Each of the firewalls 150 and 160 can also perform network address translation (NAT). In one embodiment, packets go to the real-time firewall 150 first. The real-time firewall 150 receives real-time packets from the source network and forwards packets that are accepted according to some filtering characteristics described in the corresponding control protocol. Packets that are rejected are then forwarded to the application firewall 160 or discarded or dumped. The application firewall 160 can apply more complex analysis such as stateful inspection to determine if the packets should be allowed in or out.

Figure 2 is a diagram illustrating the real-time firewall 150 shown in Figure 1 according to one embodiment of the invention. The real-time firewall 150 includes a controller 210, a filter 230, and a modifier 250. The controller 210, the filter 230, and the modifier 250 may be implemented by hardware, software, firmware or any combination thereof. Hardware, software, or firmware implementation may be represented by modules. Module coupling may include physical connections, common memory, message passing, parameter and/or argument passing, or any technique that allows information from one module to be transferred to another module.

The controller 210 specifies a filtering characteristic 215 based on the control protocol 135 or 195 from the call server 130 or 190. The call server 130 or 190 is shown in Figure 1 and is used to serve the firewall 140 between the

networks 110 and 170. At any time, one of the networks 110 and 170 is a source network and the other is a destination network. The controller 210 further specifies a modifying action 255 based on the control protocol 135 or 195.

The filtering characteristic 215 characterizes the packets to be received or transmitted from the end system 120 or 180 (Figure 1). The filtering characteristic 215 may be any one of a traffic characteristic, a network address, a port identifier, any combination of source and destination addresses and port numbers, or packet fields such as the presence of an RTP header, corresponding to the call at the end system 120 or 180. The call may be a voice over Internet protocol (VoIP) call, a video message, or a video/audio message.

The filter 230 is coupled to the controller 210 to filter the packet 152 or 154 in a call transmitted from the source network based on the filtering characteristic 215. The filter 230 includes an extractor 232, a matcher 234, and a packet router 236. The extractor 232 extracts a characteristic of the packet 152 or 154. The matcher 234 compares the extracted characteristic and the filtering characteristic 215 and generates a matching result. The packet router 236 routes the packet 152/154 to the modifier 250 as an accepted packet 260 if the packet 152/154 satisfies the filtering characteristic 215 (e.g., the matcher 234 generates a matching result between the extracted characteristic and the filtering characteristic 215). The packet router 236 routes the packet 152/154 to the application firewall 160 or merely dumps the packet as a rejected packet 270 if the packet 152/154 does not satisfy the filtering characteristic 215 (e.g., the matcher 234 generates a non-matching result between the extracted characteristic and the filtering characteristic 215). The rejected packet 270 may be further processed by the application firewall 160 to determine if the packet can be further accepted or rejected by the firewall.

The modifier 250 is coupled to the controller 210 and the filter 230 to modify the accepted packet 260 based on the modifying action 255. Then the modified packet is sent to the destination network. The modifying action 255 may be one of an address swapping, a port swapping, a network address translation (NAT), and a protocol conversion. The protocol conversion may be a conversion

from Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6), or vice versa.

The control protocol 135/195 may be any appropriate protocol. Examples of the control protocol 135/195 include Media Gateway Control (Megaco) protocol and the Common Open Policy Service (COPS) protocol, especially the COPS for Policy Provisioning (COPS-PR).

The COPS is supported at many routers and by policy servers. The COPS messages are transported over a secure TCP connection. The COPS message sequence typically consists of a request (REQ) message and a decision (DEC) message. The REQ message is sent from the real-time firewall 150 to the call server 130/190 to request filtering information. The DEC message is sent from the call server 130/190 to the real-time firewall 150 to contain filtering information including the filtering characteristic 215. The objects carried in the COPS message may include Policy Rule Identifier (PRID) objects, Encoded Policy Instance Data (EPD) objects, and optional extensions. The PRID objects reference one or more specific filtering rules (e.g., traffic bandwidth, IP address or port number corresponding to the call). The EPD objects carry an encoded value comprising a policy or a filtering rule. The extensions may include information on network address translation (NAT) or protocol conversion (e.g., between IPv4 and IPv6).

Figure 3 is a flowchart illustrating a process 300 for real-time media communication across firewall according to one embodiment of the invention. Note that the order of the processing blocks is merely for illustrative purposes. The order of operations may be changed as appropriate.

Upon START, the user initiates a call at the end system (Block 310). This call may include a VoIP, a video message, a video/audio message, or any media message or communication. Then, the end system contacts the corresponding call server to get authorization to make the call according to the call setup protocol (Block 315). Next, the call server downloads the filtering information, including a filtering characteristic, and/or modifying action to the real-time firewall using a control protocol (Block 320). The call server then authorizes the end system to

begin sending real-time packets for the call (Block 325). Upon receipt of the authorization from the call server, the end system sends real-time packets to the real-time firewall (Block 330). Then, the filter in the real-time firewall checks the packets against the filtering characteristic and other criteria (Block 335).

Next, it is determined if the packet matches the filtering characteristic (Block 340). If not, the packet is rejected and is forwarded to the application firewall or is discarded (Block 345). The process 300 is then terminated. Otherwise, if the packet satisfies the filtering characteristic, it is accepted and is forwarded to the modifier (Block 350). Then, the modifier optionally adds a modifying action (e.g., swap addresses, swap port numbers, convert protocol) to the accepted packet (Block 355). The modifier then forwards the modified packet to the destination network (Block 360). The process 300 is then permitted.

While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the invention, which are apparent to persons skilled in the art to which the invention pertains are deemed to lie within the spirit and scope of the invention.